EXHIBIT A

UNITED STATES DISTRICT COURT

for the

Southern District of New York

16 MAG 4000

In the Matter of the Search of
(Briefly describe the property to be searched or identify the person by name and address)

THE OFFICE OF PLATINUM PARTNERS, L.P.
(SEE ATTACHMENT A)

Case No.

APPLICATION FOR A SEARCH WARRANT

I, a federal law enforcement officer or an attorney for the government, request a search warrant and state under penalty of perjury that I have reason to believe that on the following person or property *(identify the person or describe the property to be searched and give its location)*:

THE OFFICE OF PLATINUM PARTNERS, L.P., LOCATED ON THE 14th FLOOR OF 250 WEST 55th STREET, NEW YORK, NY, AND INSIDE THE LOCKED AND CLOSED CONTAINERS OR ITEMS CONTAINED THEREIN

located in the Southern District of New York, there is now concealed *(identify the person or describe the property to be seized)*:

PLEASE SEE ATTACHED AFFIDAVIT AND ATTACHMENTS.

The basis for the search under Fed. R. Crim. P. 41(c) is *(check one or more)*:

- ☑ evidence of a crime;
- ☑ contraband, fruits of crime, or other items illegally possessed;
- ☑ property designed for use, intended for use, or used in committing a crime;
- ☐ a person to be arrested or a person who is unlawfully restrained.

The search is related to a violation of:

Code Section	*Offense Description*
15 U.S.C. §§ 78j(b) and 78ff	Securities Fraud
18 U.S.C. §§ 1956 and 1957	Money Laundering
18 U.S.C. §§ 1341, 1343, 1349	Mail Fraud, Wire Fraud and Conspiracy

The application is based on these facts:

PLEASE SEE ATTACHED AFFIDAVIT AND ATTACHMENTS.

☑ Continued on the attached sheet.

☐ Delayed notice of ____ days (give exact ending date if more than 30 days: _____) is requested under 18 U.S.C. § 3103a, the basis of which is set forth on the attached sheet.

[redacted]
Applicant's signature

Craig Minsky, Special Agent, FBI
Printed name and title

Sworn to before me and signed in my presence.

Date: 06/21/2016

S/Debra Freeman
Judge's signature

City and state: New York, New York

Hon. Debra Freeman, Chief U.S.M.J., S.D.N.Y.
Printed name and title

ATTACHMENT A 16 MAG 4000

Property to be searched

The property to be searched is **THE OFFICE OF PLATINUM PARTNERS, L.P., LOCATED ON THE 14th FLOOR OF THE OFFICE BUILDING LOCATED AT 250 WEST 55th STREET, NEW YORK, NEW YORK 10019, AND INSIDE THE LOCKED AND CLOSED CONTAINERS OR ITEMS CONTAINED THEREIN.**

WMP/AC

UNITED STATES DISTRICT COURT
SOUTHERN DISTRICT OF NEW YORK

----------X

IN THE MATTER OF THE APPLICATION OF THE UNITED STATES OF AMERICA FOR A SEARCH WARRANT FOR THE PREMISES KNOWN AND DESCRIBED AS THE OFFICE OF PLATINUM PARTNERS, L.P., LOCATED ON THE 14th FLOOR OF THE OFFICE BUILDING LOCATED AT 250 WEST 55th STREET, NEW YORK, NEW YORK 10019, AND INSIDE THE LOCKED AND CLOSED CONTAINERS OR ITEMS CONTAINED THEREIN

TO BE FILED UNDER SEAL

AFFIDAVIT IN SUPPORT OF APPLICATION FOR SEARCH WARRANT

----------X

SOUTHERN DISTRICT OF NEW YORK, SS:

I, CRAIG MINSKY, being duly sworn, depose and state:

I. Introduction

1. I am a Special Agent with the Federal Bureau of Investigation ("FBI"), duly appointed by law and acting as such.

2. I make this affidavit in support of an application under Rule 41 of the Federal Rules of Criminal Procedure for a warrant to search the premises known as THE OFFICE OF PLATINUM PARTNERS, L.P., LOCATED ON THE 14th FLOOR OF THE OFFICE BUILDING LOCATED AT 250 WEST 55th STREET, NEW YORK, NEW YORK 10019, AND INSIDE THE LOCKED AND CLOSED CONTAINERS OR ITEMS CONTAINED THEREIN (hereinafter, the "SUBJECT PREMISES"), which is more particularly described in Attachment A, for the things described in Attachment B.

3. I have been a Special Agent with the FBI since 2006. Since July 2014, I have been assigned to Squad C-35, one of the FBI's securities and corporate fraud units, which focuses its investigations on securities fraud, mail fraud, and wire fraud offenses. In my capacity as an FBI Special Agent, I have participated in numerous investigations into securities fraud, mail fraud, wire fraud, and money laundering, during the course of which I have conducted or participated in surveillance, execution of search warrants and arrest warrants, and debriefings of victims, informants, and cooperating witnesses. Based on my training and experience, I am aware that individuals committing fraud commonly use computers and electronic devices in furtherance of their criminal activities, including but not limited to, communications by electronic mail and text messages. I am also aware that office space used to commit fraud commonly contains paper records used in furtherance of criminal activities, including but not limited to, solicitation documents, statements, agreements, invoices, bank records and phone records. As a result of my training and experience, I am familiar with the techniques and methods of operation used by individuals involved in criminal activity to conceal their activities from detection by law enforcement authorities.

4. I have personally participated in the investigation of the offenses discussed below. I am familiar with the facts and circumstances of this investigation from: (a) my personal participation in this investigation, (b) reports made to me by other law enforcement authorities, (c) interviews with witnesses and victims, and (d) review of emails, text messages, solicitation documents, corporate agreements, bank records, and other documents.

5. The FBI and the United States Postal Inspection Service ("USPIS") are investigating violations of criminal law by the managers, principal partners and employees of Platinum Partners, L.P. ("Platinum"), a New York hedge fund firm that purportedly managed

more than $1.2 billion in assets. As set forth below, I submit that there is probable cause to believe that presently contained within the SUBJECT PREMISES is evidence, fruits and instrumentalities of criminal offenses, to wit: securities fraud, in violation of Title 15, United States Code, Sections 78j(b) and 78ff, and Title 18, United States Code, Section 1348; mail fraud, in violation of Title 18, United States Code, Section 1341; wire fraud, in violation of Title 18, United States Code, Section 1343; conspiracy to commit the above offenses, in violation of Title 18, United States Code, Sections 371 and 1349; money laundering and money laundering conspiracy, in violation of Title 18, United States Code, Sections 1956 and 1957; and violations of the Internal Revenue Laws (codified in Title 26 of the United States Code).

6. [redacted]. However, on June 14, 2016, the Wall Street Journal reported that Platinum told investors that it intends to unwind its main hedge fund. Platinum did not inform the government or the SEC about the unwinding of this fund prior to the announcement and the Wall Street Journal article. Additionally, a cooperating witness ("CW-1"), a former Platinum employee whose identity is known to your affiant, has informed me that a current Platinum employee told him that Platinum intends to use assets from the unwinding of its main hedge fund to repay other funds rather than satisfy redemptions from investors in the main fund. Moreover, despite concerns raised by the government, Platinum is currently represented by the same outside law firm and lawyer who represents Mark Nordlicht, Platinum's founder and

Chief Investment Officer, who is primarily responsible for the alleged fraud described below. [redacted]

7. This affidavit is intended to show only that there is sufficient probable cause for the requested warrant and does not set forth all of my knowledge about this matter.

II. Probable Cause

8. The facts set forth below establish probable cause to believe that from at least 2010 to the present, in the Southern District of New York, the Eastern District of New York and elsewhere, Mark Nordlicht, [redacted], [redacted], David Levy, Daniel Small, [redacted] and [redacted], together with others, engaged in a scheme to defraud investors and potential investors in Platinum through material misrepresentations and omissions about, among other things, the performance, liquidity, ownership, control, and use of investments of Platinum's funds.

A. The Relevant Entities

9. Platinum, a hedge fund based in New York, New York, brands itself as a specialist in distressed investments that purportedly manages more than $1.2 billion in assets. Platinum, through Platinum Management (NY) LLC, is an investment adviser registered with the SEC. Platinum manages several funds, but the vast majority of its assets are invested in the Platinum Partners Value Arbitrage Fund, L.P. ("PPVA") and the Platinum Partners Credit Opportunity Fund, L.P. ("PPCO"). The principals of Platinum also controlled Beechwood Asset Management ("BAM") and Beechwood Bermuda International Ltd. ("BBIL").

10. PPVA, established in 2003, is Platinum's signature fund and acts as a master fund that is comprised of the following feeder funds: (i) Platinum Partners Value

Arbitrage Fund (USA) LP ("Onshore Fund"); (ii) Platinum Partners Value Arbitrage Fund (International) Ltd. ("Offshore Fund"); and (iii) Platinum Partners Value Arbitrage Intermediate Fund Ltd. ("Intermediate Fund"). PPVA is composed primarily of illiquid assets and penny stocks, with a significant emphasis on exploration- and developmental-stage energy companies.

11. Black Elk Energy Offshore Operations, LLC ("Black Elk"), formed in November 2007, is an oil and natural gas company based in Houston, Texas that is engaged in the exploration, development, production and exploitation of oil and natural gas properties. Black Elk was formed through a series of acquisitions funded through the issuance of $150 million in 13.75% high yield public bonds. Its business was to acquire oil and natural gas producing properties within the Outer Continental Shelf of the United States in the Gulf of Mexico. Platinum controlled Black Elk. As of March 2014, PPVA valued Black Elk as worth between $144 million and $186 million.

12. Golden Gate Oil, LLC ("Golden Gate"), formed by Platinum through a joint venture in April 2012, is a mid-coast onshore oil and gas exploration and production company based in Santa Maria, California. According to its website, Golden Gate purportedly planned to grow its onshore portfolio through acquisitions and organic prospect generation in the lower forty-eight states as future cash flow dictates, in addition to the existing horizontal Monterey shale drilling program that is in progress. Platinum controls Golden Gate. As of March 2014, PPVA valued Golden Gate as worth between $144 million and $176 million.

B. The Relevant Individuals

13. Mark Nordlicht, a resident of New Rochelle, New York, is one of the founders, a part owner, and the Chief Investment Officer ("CIO") of Platinum. Nordlicht was primarily responsible for Platinum's investment decisions and the valuation of its assets.

14. [redacted], a resident of [redacted], New York, is one of the founders, an investor, and a secret part-owner of Platinum.[1] [redacted]'s association with Platinum was hidden from a number of investors, yet [redacted] was also heavily involved in soliciting investments for Platinum.

15. [redacted], a resident of [redacted], New York, is one of the founders, an investor, and a secret part-owner of Platinum. Together with [redacted], [redacted] also formed Centurion Credit Management, LP, which in 2011, was merged into Platinum and named PPCO.

16. David Levy, a resident of New York, New York, is the co-Chief CIO of Platinum. Between 2012 and 2015, Levy served as the co-portfolio manager for Black Elk and B Asset Manager LP.

17. Daniel Small, a resident of New York, New York, was employed by Platinum from 2007 to July 2015. Small was a managing director and co-portfolio manager for Black Elk.

18. [redacted], a resident of [redacted], New York, was employed by Platinum from approximately February 2008 to December 2015. [redacted] worked for PPCO, and in 2013, served as the Chief Financial Officer of PPCO. In 2014, [redacted] became the Chief Operating Officer for Platinum.

C. The Fraudulent PPVA Valuation Scheme

19. According to Platinum, since inception through October 2015, PPVA has

---

[1] On June 8, 2016, [redacted] was arrested by the FBI and charged by the U.S. Attorney's Office for the Southern District of New York with committing honest services wire fraud, in connection with [redacted]'s payment of a $60,000 bribe to [redacted], the President of the Correction Officers' Benevolent Association ("COBA"), and the promise of

returned 17% annually, with positive returns in 84% of all months and without ever having a year with negative returns. In a November 2015 investor presentation, Platinum reported that PPVA had approximately $775 million in assets under management ("AUM"). A PPVA portfolio valuation report, prepared by Sterling Valuation Group Inc. ("Sterling") in March 2014, provided that PPVA's portfolio had twenty-seven positions that purportedly ranged in value from $630 million to $735 million. In 2015, Platinum provided investors with fact sheets for PPVA's Offshore Fund and Onshore Fund that showed positive returns in each year for each fund from 2003 through 2015 and a cumulative return for each fund of more than 600%. Platinum touted to investors and potential investors Sterling's valuations, which supported PPVA's consistently high returns.

20. Platinum's fraudulent overvaluations of PPVA's assets in 2014 and thereafter is revealed by an analysis of its two largest positions, namely, Black Elk and Golden Gate. As of March 31, 2014, in PPVA's portfolio valuation report, Platinum represented to investors that Black Elk and Golden Gate were each worth between $144 million and $176 million. Black Elk and Golden Gate, which accounted for approximately 50% of PPVA's total stated value in 2014, were failing energy companies that lost most of their value after 2014. Despite this, Platinum claimed that PPVA's AUM remained steady – approximately $775 million – through 2015. A simple objective analysis of the energy industry reveals that Platinum's valuation of PPVA in November 2015, which remained, at worst, steady, defies logic. Specifically, the price of crude oil, which directly impacted more than 50% of PPVA's portfolio, crashed from $107.26 per barrel on June 20, 2014 to $46.59 per barrel on October 30, 2015, but as noted above, it had essentially no impact on PPVA's valuation of its AUM. Indeed,

---

future bribe payments, in exchange for [redacted]'s investment of $20 million of COBA money in

Platinum's marketing materials claimed that PPVA's Offshore Fund returned more than 9% over essentially the same time period (from June 2014 through August 2015). Platinum's valuations in November 2015 to investors are further contradicted by the following simple facts: (i) Golden Gate's wells collectively produced only $1 million in estimated revenues in 2014, based on data compiled by the California Department of Conservation; and (ii) federal prosecutors charged Black Elk and its contractors in August 2015 with a number of federal crimes related to a 2012 fatal explosion and fire at a Black Elk oil well in the Gulf of Mexico, resulting in Black Elk going through bankruptcy proceedings and court approved restructuring.

21. Platinum's misrepresentations about Black Elk's performance were confirmed by Employee 1, a former Black Elk officer whose identity is known to your affiant. Employee 1 described how Platinum, led by Nordlicht, Levy and Small, controlled Black Elk's decisions and its Board of Directors. Employee 1 informed me that Black Elk had no positive cash flow or net profit in 2013 or 2014, and few assets in 2015 following the sale of its best assets in August 2014 to Renaissance Offshore, LLC ("Renaissance"). Indeed, Employee 1 stated that from approximately 2012 through 2014, Black Elk was not generating sufficient revenue and could barely pay its vendors and creditors.

22. Platinum's misrepresentations about PPVA's performance were also corroborated by CW-1. Specifically, CW-1 informed your affiant that, in 2015, PPVA was not generating positive cash flow, and by March 2015, Platinum did not have the necessary assets to fulfill the majority of investor redemptions in PPVA. CW-1 also confirmed that Golden Gate was not generating any profits in 2015. Consequently, CW-1 stated that Nordlicht used new investor funds and transferred funds from other entities, including PPCO, to pay select investors

---

Platinum.

seeking redemptions. When CW-1 questioned Nordlicht about using new investor funds and funds from other entities to pay old investors, Nordlicht plainly stated that it is a "big stew." And when CW-1 warned Nordlicht that it was improper to selectively choose investors for redemptions and that the investors who did not get paid would complain to the SEC, Nordlicht responded, in sum and substance, that the investors would not complain to the SEC because he had created a scenario of a "mutually assured destruction" and investors knew that complaining to the SEC meant that they would only receive ten to twenty cents on the dollar. Additionally, CW-1 explained that Platinum profited greatly from its fraudulent overvaluations because it withdrew its 20% performance fee annually based on its fraudulent valuations and not on actual realized gains from its investments.

23. I have also spoken to Investor 1, a PPVA investor whose identity is known to your affiant, who has confirmed that he has been unable to redeem approximately $1.8 million of his investment in PPVA. Specifically, Investor 1 stated that he invested in PPVA in approximately 2008 because it purported to be a diversified hedge fund that had high performance and liquidity, i.e., fulfilled redemptions within sixty to ninety days. Although Investor 1 was able to redeem his investments prior to 2015, albeit with some delays, he experienced issues with redemptions in 2015. In January 2015, Investor 1 submitted a redemption request for $500,000 in order to take out some gains and diversify his overall investment portfolio. In April 2015, as the redemption was due, [redacted], Platinum's Chief Marketing Director, called Investor 1 and advised him to defer his redemption to the next quarter as Platinum was expecting April to be a "big month." Based on this information, Investor 1 deferred his redemption to June 2015, and was ultimately able to redeem $500,000 in June 2015. Investor 1's statement revealed that PPVA did in fact have a "big month" in April

2015, returning 7% for the month. In the summer of 2015, Nordlicht and [redacted] visited Investor 1 and another investor at their offices to offer investments in a class of shares that were less liquid. Because Investor 1 was not interested in a less liquid investment, he declined Nordlicht and [redacted]'s offer, but this offer combined with Platinum's divining of a big month in April 2015 raised red flags for Investor 1 that caused him to make another redemption request for $800,000 in September 2015. The $800,000 redemption was due, by the latest, on February 1, 2016. But, as of June 20, 2016, Investor 1 had not yet received the $800,000 that he requested in September 2015, and Platinum stopped responding to his emails in May 2016.

24. Platinum Management (NY) LLC's bank records for 2014 and 2015 at Sterling National Bank reveal that its primary account started with a $124,997.53 balance on January 1, 2014 and ended with a $171,432.38 balance on December 31, 2015. This is particularly odd given the fact that a total of approximately $85 million was deposited and a total of approximately $85 million was withdrawn during this period; the monthly deposits and withdrawals were essentially identical.

25. Similarly, PPVA's bank records for 2015 at Sterling National Bank reveal that its primary account started with a $1,415,937.55 balance on January 1, 2015 and ended with a $1,245,465.16 balance on December 31, 2015. Once again, this is particularly odd given the fact that a total of approximately $448 million was deposited and a total of approximately $448 million was withdrawn during this period; the monthly deposits and withdrawals were essentially identical.

26. Based on the above-described investigation and my training and experience, there is probable cause to believe that Platinum has lied to investors and potential investors about the performance of its funds and the true value of its assets, specifically, PPVA

and PPCO. Additionally, there is also probable cause to believe that Nordlicht, his partners and managers operated Platinum as a Ponzi scheme and co-mingled and transferred funds between various entities to conceal the true nature and performance of the various funds.

D. The Fraudulent Black Elk Bond Consent Solicitation

27. Employee 1, the former Black Elk officer referenced above, also described a fraud perpetrated by Platinum against some of Black Elk's holders of the 13.75% senior secured notes that were issued on November 23, 2010 and that matured on December 31, 2015. In the first quarter of 2013, Platinum invested $50 million into Black Elk in exchange for 100% of the Series E Preferred Stock Interest, which paid interest in kind at a rate of 20% escalating to 36% if it was not paid back on time. The funds were used towards an unsuccessful exploration program that left Black Elk in a difficult financial situation. As Black Elk was negotiating the sale of a substantial portion of Black Elk assets to Renaissance for $170 million to pay Black Elk's bond holders, Platinum devised a plan to pay the preferred equity holders ahead of the bond holders by proposing a tender offer and consent solicitation. Employee 1 questioned Platinum's proposal because it defied logic that a reasonable bond holder would not tender but consent to allow a class of equity to move ahead of him or her and take the proceeds from his or her collateral. In response, Platinum told Employee 1, in sum and substance, to take their word that a majority of the bond holders would consent to the equity distribution.

28. On July 16, 2014, Black Elk announced that it had commenced a cash tender offer to purchase its outstanding $150 million aggregate principal amount of the 13.75% bonds due in 2015 (the "Consent Solicitation"). In the Consent Solicitation, on page 5, Black Elk disclosed that "[PPVA] and its affiliates, which own approximately 85% of our outstanding voting membership interests, own approximately $18,321,000 principal amount of the

outstanding Notes." The offer expired on August 13, 2014 and was contingent on the sale to Renaissance. As the offer expired on August 13, 2014, the holders of $11,333,000 of the bonds validly tendered and were paid. Surprisingly, the holders of $110,565,000 or 73.71% of the bonds validly consented to the Consent Solicitation.

29. Unbeknownst to Employee 1 at that time, Platinum and its affiliates beneficially owned or controlled $98,631,000 of the bonds (not merely $18,321,000). Platinum's control of $98,631,000 accounted for 65.75% of the 73.71% of bond holders who consented. Platinum concealed this information from Employee 1 and from the rest of the bond holders. Indeed, in an email dated July 8, 2014, prior to the Consent Solicitation announcement, [redacted] sent an email to Levy and Small and attached a spreadsheet listing Black Elk's public bond holdings. The attached spreadsheet, entitled "BlackElk Bond Holders," listed the following entities and their holdings: (i) PPCO: $29,582,000; (ii) PPVA: $18,321,000; (iii) PPLO (Platinum Partners Liquid Opportunity Fund, L.P.): $13,711,000; (iv) BAM: $13,360,000; (v) BBIL: $23,657,000; and (vi) Total: $98,631,000. Despite this knowledge, on August 14, 2014, Small sent an email to [redacted] and Employee 1, wherein Small confirmed, in part, that PPVA and its affiliates only controlled $18,321,000 of the bonds.

30. I have spoken to a number of bond holders who did not consent and whose senior secured bonds are now worthless. Most of them did not recall hearing about the Consent Solicitation and never consented to the offer. Notably, none of the bond holders I spoke to were aware that Platinum controlled $98,631,000 or 65% of the bonds and that Platinum had devised the idea for the Consent Solicitation because it owned 85% of the preferred equity.

31. PPVA's Black Elk bank records for 2014 and 2015 at Sterling National Bank reveal that its primary account started with a $0 balance on January 1, 2014 and ended with

a $0 balance on December 31, 2015. Strangely, the monthly ending balance during this period, with the exception of December 31, 2014 when it was $71,140.69, never exceeded $8,000. This is particularly odd given the fact that a total of approximately $112 million was deposited and a total of approximately $112 million was withdrawn during this period; the monthly deposits and withdrawals were essentially identical.

E. Relevant Facts Concerning the Subject Premises

32. CW-1, who visited the SUBJECT PREMISES earlier this month, informed me that Platinum now has sublet the east wing of the SUBJECT PREMISES to unknown entities and individuals, but continues to maintain office space on the west wing of the SUBJECT PREMISES (facing Eighth Avenue). When you get off the elevator on the 14th floor, you see the reception area behind glass doors and a "Platinum Partners" sign behind the reception area. You can then proceed towards either the right or the left of the reception area into the main office area.

33. CW-1 stated that Platinum has drawers and file cabinets in individual offices and in the general area and that there is a room towards the back of the office space that contains file cabinets and that may also contain Platinum's computer servers. CW-1 also told me that Platinum assigned desktop computers to all employees and laptop computers and iPads to select high-level employees. Finally, CW-1 noted that Nordlicht is a prolific user of his iPad, which he uses for business purposes even while sitting at his desk.

III. Technical Terms

34. Based on my training and experience, I use the following technical terms to convey the following meanings:

a. *IP Address*: The Internet Protocol address (or simply "IP address") is a unique numeric address used by computers on the Internet. An IP address looks like a series of four numbers, each in the range 0-255, separated by periods (e.g., 121.56.97.178). Every computer attached to the Internet must be assigned an IP address so that Internet traffic sent from and directed to that computer may be directed properly from its source to its destination. Most Internet service providers control a range of IP addresses. Some computers have static—that is, long-term—IP addresses, while other computers have dynamic—that is, frequently changed—IP addresses.

b. *Internet*: The Internet is a global network of computers and other electronic devices that communicate with each other. Due to the structure of the Internet, connections between devices on the Internet often cross state and international borders, even when the devices communicating with each other are in the same state.

c. *Storage medium*: A storage medium is any physical object upon which computer data can be recorded. Examples include hard disks, RAM, floppy disks, flash memory, CD-ROMs, and other magnetic or optical media.

IV. Computers, Electronic Storage and Forensic Analysis

35. As described above and in Attachment B, this application seeks permission to search for records that might be found on the SUBJECT PREMISES, in whatever form they are found. One form in which the records might be found is data stored on a computer's hard drive, iPads or other storage media. Thus, the warrant applied for would authorize the seizure of electronic storage media or, potentially, the copying of electronically stored information, all under Rule 41(e)(2)(B).

36. *Probable cause.* I submit that if a computer or storage medium is found

on the SUBJECT PREMISES, there is probable cause to believe those records will be stored on that computer or storage medium, for at least the following reasons:

a. Based on my knowledge, training, and experience, I know that computer files or remnants of such files can be recovered months or even years after they have been downloaded onto a storage medium, deleted, or viewed via the Internet. Electronic files downloaded to a storage medium can be stored for years at little or no cost. Even when files have been deleted, they can be recovered months or years later using forensic tools. This is so because when a person "deletes" a file on a computer, the data contained in the file does not actually disappear; rather, that data remains on the storage medium until it is overwritten by new data.

b. Therefore, deleted files, or remnants of deleted files, may reside in free space or slack space—that is, in space on the storage medium that is not currently being used by an active file—for long periods of time before they are overwritten. In addition, a computer's operating system may also keep a record of deleted data in a "swap" or "recovery" file.

c. Wholly apart from user-generated files, computer storage media—in particular, computers' internal hard drives—contain electronic evidence of how a computer has been used, what it has been used for, and who has used it. To give a few examples, this forensic evidence can take the form of operating system configurations, artifacts from operating system or application operation, file system data structures, and virtual memory "swap" or paging files. Computer users typically do not erase or delete this evidence, because special software is typically required for that task. However, it is technically possible to delete this information.

d. Similarly, files that have been viewed via the Internet are sometimes automatically downloaded into a temporary Internet directory or "cache."

e. Based on information from CW-1 and former employees of Platinum, and actual inspection of other evidence related to this investigation, such as spreadsheets, financial records and invoices, I am aware that computer equipment was used to generate, store, and print documents used in the above-described scheme. As described above, there is reason to believe that there is a computer system currently located on the SUBJECT PREMISES.

37. *Forensic evidence.* As further described in Attachment B, this application seeks permission to locate not only computer files that might serve as direct evidence of the crimes described on the warrant, but also forensic electronic evidence that establishes how computers were used, the purpose of their use, who used them, and when. There is probable cause to believe that this forensic electronic evidence will be on any storage medium in the SUBJECT PREMISES because:

a. Data on the storage medium can provide evidence of a file that was once on the storage medium but has since been deleted or edited, or of a deleted portion of a file (such as a paragraph that has been deleted from a word processing file). Virtual memory paging systems can leave traces of information on the storage medium that show what tasks and processes were recently active. Web browsers, e-mail programs, and chat programs store configuration information on the storage medium that can reveal information such as online nicknames and passwords. Operating systems can record additional information, such as the attachment of peripherals, the attachment of USB flash storage devices or other external storage media, and the times the computer was in use. Computer file systems can record information

about the dates files that were created and the sequence in which they were created, although this information can later be falsified.

b. As explained herein, information stored within a computer and other electronic storage media may provide crucial evidence of the "who, what, why, when, where, and how" of the criminal conduct under investigation, thus enabling the United States to establish and prove each element or alternatively, to exclude the innocent from further suspicion. In my training and experience, information stored within a computer or storage media (e.g., registry information, communications, images and movies, transactional information, records of session times and durations, internet history, and anti-virus, spyware, and malware detection programs) can indicate who has used or controlled the computer or storage media. This "user attribution" evidence is analogous to the search for "indicia of occupancy" while executing a search warrant at a residence. The existence or absence of anti-virus, spyware, and malware detection programs may indicate whether the computer was remotely accessed, thus inculpating or exculpating the computer owner. Further, computer and storage media activity can indicate how and when the computer or storage media was accessed or used. For example, as described herein, computers typically contain information that logs: computer user account session times and durations, computer activity associated with user accounts, electronic storage media that connected with the computer, and the IP addresses through which the computer accessed networks and the internet. Such information allows investigators to understand the chronological context of computer or electronic storage media access, use, and events relating to the crime under investigation. Additionally, some information stored within a computer or electronic storage media may provide crucial evidence relating to the physical location of other evidence and the suspect. For example, images stored on a computer may both show a particular location

and have geolocation information incorporated into its file data. Such file data typically also contains information indicating when the file or image was created. The existence of such image files, along with external device connection logs, may also indicate the presence of additional electronic storage media (e.g., a digital camera or cellular phone with an incorporated camera). The geographic and timeline information described herein may either inculpate or exculpate the computer user. Last, information stored within a computer may provide relevant insight into the computer user's state of mind as it relates to the offense under investigation. For example, information within the computer may indicate the owner's motive and intent to commit a crime (e.g., internet searches indicating criminal planning), or consciousness of guilt (e.g., running a "wiping" program to destroy evidence on the computer or password protecting/encrypting such evidence in an effort to conceal it from law enforcement).

c. A person with appropriate familiarity with how a computer works can, after examining this forensic evidence in its proper context, draw conclusions about how computers were used, the purpose of their use, who used them, and when.

d. The process of identifying the exact files, blocks, registry entries, logs, or other forms of forensic evidence on a storage medium that are necessary to draw an accurate conclusion is a dynamic process. While it is possible to specify in advance the records to be sought, computer evidence is not always data that can be merely reviewed by a review team and passed along to investigators. Whether data stored on a computer is evidence may depend on other information stored on the computer and the application of knowledge about how a computer behaves. Therefore, contextual information necessary to understand other evidence also falls within the scope of the warrant.

e. Further, in finding evidence of how a computer was used, the purpose of its use, who used it, and when, sometimes it is necessary to establish that a particular thing is not present on a storage medium. For example, the presence or absence of counter-forensic programs or anti-virus programs (and associated data) may be relevant to establishing the user's intent.

38. *Necessity of seizing or copying entire computers or storage media.* In most cases, a thorough search of a premises for information that might be stored on storage media often requires the seizure of the physical storage media and later off-site review consistent with the warrant. In lieu of removing storage media from the premises, it is sometimes possible to make an image copy of storage media. Generally speaking, imaging is the taking of a complete electronic picture of the computer's data, including all hidden sectors and deleted files. Either seizure or imaging is often necessary to ensure the accuracy and completeness of data recorded on the storage media, and to prevent the loss of the data either from accidental or intentional destruction. This is true because of the following:

a. The time required for an examination. As noted above, not all evidence takes the form of documents and files that can be easily viewed on site. Analyzing evidence of how a computer has been used, what it has been used for, and who has used it requires considerable time, and taking that much time on the Premises could be unreasonable. As explained above, because the warrant calls for forensic electronic evidence, it is exceedingly likely that it will be necessary to thoroughly examine storage media to obtain evidence. Storage media can store a large volume of information. Reviewing that information for things described in the warrant can take weeks or months, depending on the volume of data stored, and would be impractical and invasive to attempt on-site.

b. Technical requirements. Computers can be configured in several different ways, featuring a variety of different operating systems, application software, and configurations. Therefore, searching them sometimes requires tools or knowledge that might not be present on the search site. The vast array of computer hardware and software available makes it difficult to know before a search what tools or knowledge will be required to analyze the system and its data on the Premises. However, taking the storage media off-site and reviewing it in a controlled environment will allow its examination with the proper tools and knowledge.

c. Variety of forms of electronic media. Records sought under this warrant could be stored in a variety of storage media formats that may require off-site reviewing with specialized forensic tools.

39. *Nature of examination.* Based on the foregoing, and consistent with Rule 41(e)(2)(B), the warrant I am applying for would permit seizing, imaging, or otherwise copying storage media that reasonably appear to contain some or all of the evidence described in the warrant, and would authorize a later review of the media or information consistent with the warrant. The later review may require techniques, including but not limited to computer-assisted scans of the entire medium, that might expose many parts of a hard drive to human inspection in order to determine whether it is evidence described by the warrant.

40. Because Platinum has now sublet the east wing of the 14th floor of the SUBJECT PREMISES to other companies and individuals, it is possible that the SUBJECT PREMISES will contain storage media that are predominantly used, and perhaps owned, by persons who are not suspected of a crime. If it is nonetheless determined that it is possible that the things described in this warrant could be found on any of those computers or storage media, the warrant applied for would permit the seizure and review of those items as well.

41. As with any search warrant, I expect that this warrant will be executed reasonably. Reasonable execution will likely involve conducting an investigation on the scene of what computers, or storage media, must be seized or copied, and what computers or storage media need not be seized or copied. Where appropriate, officers will copy data, rather than physically seize computers, to reduce the extent of disruption. If employees of Platinum so request, the agents will, to the extent practicable, attempt to provide the employees with copies of data that may be necessary or important to the continuing function of Platinum's business. If, after inspecting the computers, it is determined that some or all of this equipment is no longer necessary to retrieve and preserve the evidence, the government will return it.

V. Conclusion

42. I submit that this affidavit supports probable cause for a warrant to search the SUBJECT PREMISES described in Attachment A and seize the items described in Attachment B.

43. Furthermore, I respectfully request that this Court issue an Order sealing, until further order of this Court, all papers submitted in support of this Application, including this affidavit and the requisite inventory notice (with the exception of one copy of the warrant and the inventory notice that will be left at the SUBJECT PREMISES). I believe that sealing this document is necessary because the items and information to be seized are relevant to an ongoing investigation and not all of the targets of this investigation will be searched at this time. Based upon my training and experience, I have learned that participants in fraudulent schemes often actively search for criminal affidavits and search warrants via the Internet, and may disseminate them to other participants in the scheme as they deem appropriate. Premature

disclosure of the contents of this affidavit and related documents may have a significant and negative impact on the continuing investigation and may severely jeopardize its effectiveness.

[redacted]

CRAIG MINSKY
Special Agent, FBI

Sworn to before me this
21st day of June, 2016

S/Debra Freeman

THE HONORABLE DEBRA FREEMAN
CHIEF UNITED STATES MAGISTRATE JUDGE
SOUTHERN DISTRICT OF NEW YORK

ATTACHMENT A

Property to be searched

The property to be searched is **THE OFFICE OF PLATINUM PARTNERS, L.P., LOCATED ON THE 14th FLOOR OF THE OFFICE BUILDING LOCATED AT 250 WEST 55th STREET, NEW YORK, NEW YORK 10019, AND INSIDE THE LOCKED AND CLOSED CONTAINERS OR ITEMS CONTAINED THEREIN.**

ATTACHMENT B

Property to be seized

1. All records relating to violations of securities fraud, in violation of Title 15, United States Code, Sections 78j(b) and 78ff and Title 18, United States Code, Section 1348; mail fraud, in violation of Title 18, United States Code, Section 1341; wire fraud, in violation of Title 18, United States Code, Section 1343; conspiracy to commit the above offenses, in violation of Title 18, United States Code, Sections 371 and 1349; money laundering and money laundering conspiracy, in violation of Title 18, United States Code, Sections 1956 and 1957; and violations of the Internal Revenue Laws (codified in Title 26 of the United States Code), those violations involving managers and employees of Platinum, including but not limited to, Mark Nordlicht, [redacted], [redacted], David Levy, Daniel Small, [redacted] and [redacted], and occurring after January 1, 2010, including:

a. Organization charts of Platinum Partners and Platinum Management (NY) LLC and all its funds, affiliates, subsidiaries, and entities under its control (collectively, "Platinum").

b. List of employees and outside contractors with titles, general responsibilities, dates of employment and compensation information.

c. Any and all performance and valuation summaries or reports for Platinum, including Platinum Partners Value Arbitrage Fund, LP ("PPVA") and Platinum Partners Credit Opportunity Fund, LP ("PPCO").

d. List of all investors in Platinum, including PPVA and PPCO, along with the amount of their investment, the performance or returns on investment, amount of fees paid (with breakdown), and any redemptions.

e. Any and all communications with investors in Platinum, including PPVA and PPCO.

f. Any and all records, including communications to investors and auditors, concerning Platinum's assets under management, the investments in its portfolios, the valuation of assets, and the performance of the investments.

g. Any and all records, including communications (written or recorded), money transfers, internal memoranda and reports, audit reports and valuation reports, concerning Platinum's investments.

h. All policies, procedures, training materials and related documents.

i. Bank records for Platinum, its affiliates and subsidiaries.

2. For any computer, iPad or storage medium whose seizure is otherwise authorized by this warrant, and any computer, iPad or storage medium that contains or in which is stored records or information that is otherwise called for by this warrant (hereinafter, "COMPUTER"):

a. evidence of who used, owned, or controlled the COMPUTER at the time the things described in this warrant were created, edited, or deleted, such as logs, registry entries, configuration files, saved usernames and passwords, documents, browsing history, user profiles, email, email contacts, "chat," instant messaging logs, photographs, and correspondence;

b. evidence indicating how and when the COMPUTER was accessed or used to determine the chronological context of computer access, use, and events relating to crime under investigation and to the COMPUTER user;

c. evidence of the attachment to the COMPUTER of other storage devices or similar containers for electronic evidence;

d. evidence of counter-forensic programs (and associated data) that are designed to eliminate data from the COMPUTER;

e. evidence of the times the COMPUTER was used;

f. passwords, encryption keys, and other access devices that may be necessary to access the COMPUTER;

g. documentation and manuals that may be necessary to access the COMPUTER or to conduct a forensic examination of the COMPUTER;

h. records of or information about Internet Protocol addresses used by the COMPUTER; and

i. records of or information about the COMPUTER's Internet activity, including firewall logs, caches, browser history and cookies, "bookmarked" or "favorite" web pages, search terms that the user entered into any Internet search engine, and records of user-typed web addresses.

As used above, the terms "records" and "information" includes all forms of creation or storage, including any form of computer or electronic storage (such as hard disks or other media that can store data); any handmade form (such as writing); any mechanical form (such as printing or typing); and any photographic form (such as microfilm, microfiche, prints, slides, negatives, videotapes, motion pictures, or photocopies).

The term "computer" includes all types of electronic, magnetic, optical, electrochemical, or other high speed data processing devices performing logical, arithmetic, or storage functions, including desktop computers, notebook computers, mobile phones, tablets, server computers, and network hardware.

The term "storage medium" includes any physical object upon which computer data can be recorded. Examples include hard disks, RAM, floppy disks, flash memory, CD-ROMs, and other magnetic or optical media.